Social Engineering and Phishing Awareness Training

Objective

- **Inform and increase the awareness of all Department of Defense personnel of the dangers and threats imposed on DoD information systems as a result of “spear-phishing” emails.**

- **Instruct personnel on how to recognize these email threats while offering methods to help counter the threat.**

Social Engineering/Phishing

Phishing is a criminal activity using social engineering techniques.

“Phishers” attempt to fraudulently acquire sensitive information, such as passwords, personal information, military operations, and credit card/financial details, by masquerading as a trustworthy person or business in an electronic communication.

All Social Engineering techniques are based on flaws in human logic

Social Engineering Techniques

Top five social engineering moments on film:

- 5. *Independence Day*: Using an old space ship as cover for two humans to infiltrate the alien mother ship and upload a virus to destroy it.
- 4. *Hackers*: Dumpster diving in the target company's trash in order to obtain financial data from printouts
- 3. *War Games*: Password cracking the military computer system by studying its creator.
- 2. *Ferris Bueller's Day Off*: Faking a grandmother's death to get Ferris's girlfriend excused from school through multiple phone calls and answering machine recordings.
- 1. *Star Wars*: R2-D2 gaining access to the death star main computer and shutting down the garbage dispensers.

All of the above hacks employ a social engineering technique.

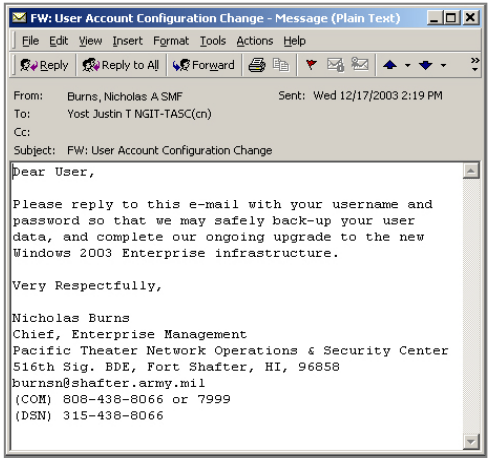
Social Engineering Techniques
Pretexing

- **Pretexting** is the act of creating an scenario to persuade a person to release information or perform an action. It most often involves some prior research or set up and the use of pieces of known information (e.g., For impersonation: Birthday, Social Security Number, last bill amount) to establish legitimacy in the mind of the target.
- Pretexting can also be used to impersonate co-workers, police, bank, IRS or insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the target. The pretexter must simply prepare answers to questions that might be asked by the target. In some cases all that is needed is a voice of the right gender, an earnest tone and an ability to think on one's feet.

Social Engineering Approaches

In-person

Telephone


FW: User Account Configuration Change - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: Burns, Nicholas A SMF
Sent: Wed 12/17/2003 2:19 PM
To: Yost Justin T NGIT-TASC(cn)
Cc:
Subject: FW: User Account Configuration Change
Dear User,
Please reply to this e-mail with your username and password so that we may safely back-up your user data, and complete our ongoing upgrade to the new Windows 2003 Enterprise infrastructure.
Very Respectfully,
Nicholas Burns
Chief, Enterprise Management
Pacific Theater Network Operations & Security Center
516th Sig. BDE, Fort Shafter, HI, 96858
burnsn@shafter.army.mil
(COM) 808-438-8066 or 7999
(DSN) 315-438-8066

E-mail

PASSWORD CHANGE ACCESS
U.S. ARMY, PACIFIC FORT SHAFTER, HAWAII
(Operated and maintained by USAG-HI DOIM)
ONE TEAM
USERNAME:
PASSWORD:
Enter your username and password then press the Enter key or click here to connect to your account.
User's Guide/Help Files
ATTENTION!
This is a DOD Computer system. Do not process, store or transmit any classified information on this system. This computer system and all related equipment, networks and network devices, including internet access are provided only for authorized U. S. Government use. DOD computer systems may be monitored for all lawful purposes, including, to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for all lawful purposes.

Websites

Social Engineering Techniques
Phishing

- Phishing
  - Phishing applies to email appearing to come from a legitimate business — a bank, or credit card company — requesting "verification" of information and warning of some dire consequence if it is not done. The letter usually contains a link to a fraudulent web page that looks legitimate — with company logos and content — and has a form requesting everything from a home address to an ATM card's PIN.
  - More recent phishing attempts have targeted the customers of banks and online payment services. E-mails supposedly from the Internal Revenue Service have also been used to glean sensitive data from U.S. taxpayers.

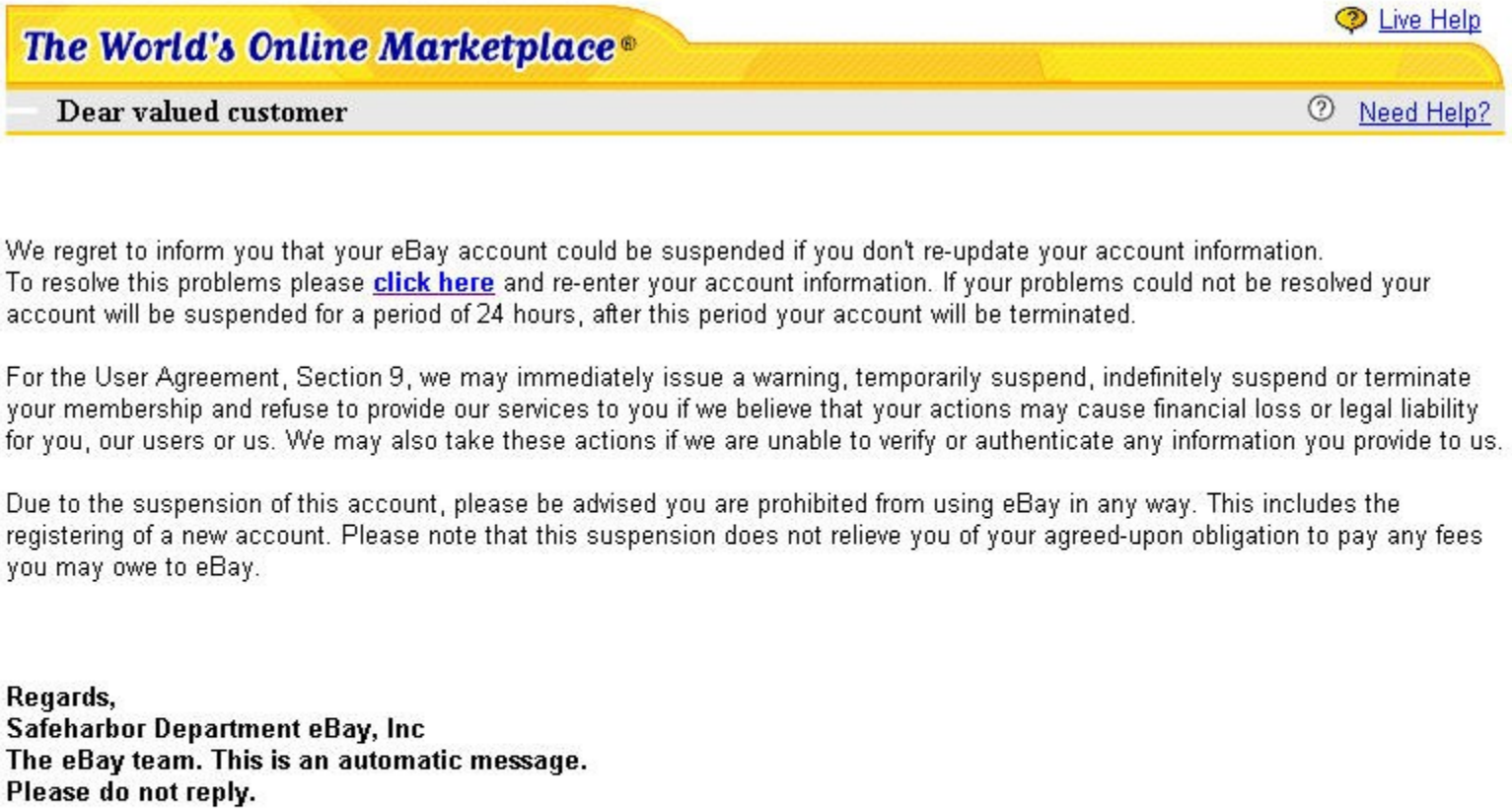
What To Look For

- Suspicious E-mail Address
- No Digital Signature
- Ambiguous Subject Lines
- Generic Message Body (Uses No Names)
- Suspicious Hyperlinks
- Suspicious Attachments (Scrutinize MS Office Files)

Beware of Phishing Schemes

Companies will never ask you to change your password through e-mail

Actual Phishing Example



The World's Online Marketplace®

Live Help

Dear valued customer

Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problems please **click here** and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team. This is an automatic message.
Please do not reply.

Announcements | Register | Shop eBay-o-rama | Security Center | Policies | PayPal
Feedback Forum | About eBay | Jobs | Affiliates Program | Developers | eBay Downloads | eBay Gift Certificates
My eBay | Site Map
Browse | Sell | Services | Search | Help | Community

Copyright Â© 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

reviewed by TRUSTe site privacy statement

Actual Phishing Example

The email does not feature a lot of Ameritrade attributes, but given the spoofed sender and the mild tone, it could be convincing:

Thank you for opening your Ameritrade® account!

Your account must be funded before you can begin trading. For details about your funding choices, log on at www.ameritrading.net and choose Help Center from the Help menu. Then click Managing your account and Deposits.

You can make the most of your Ameritrade experience by checking out Ameritrade Streamer(TM)[1], setting up your watch lists, and taking a look at everything available to you under the Research menu.

Again, thank you for choosing Ameritrade. We look forward to serving you for years to come.

Sincerely,
Kenneth I Feldman
President, Private Client Division
Ameritrade

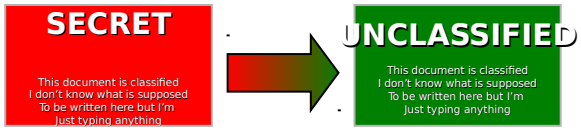
VIRTUAL UNIVERSITY
Online Classes for the Global Village

Prohibited Activities

AR 25-2

Personal Gain Or Illegal Activities

Online Gambling


SECRET
This document is classified
I don't know what is supposed
To be written here but I'm
Just typing anything
UNCLASSIFIED
This document is classified
I don't know what is supposed
To be written here but I'm
Just typing anything

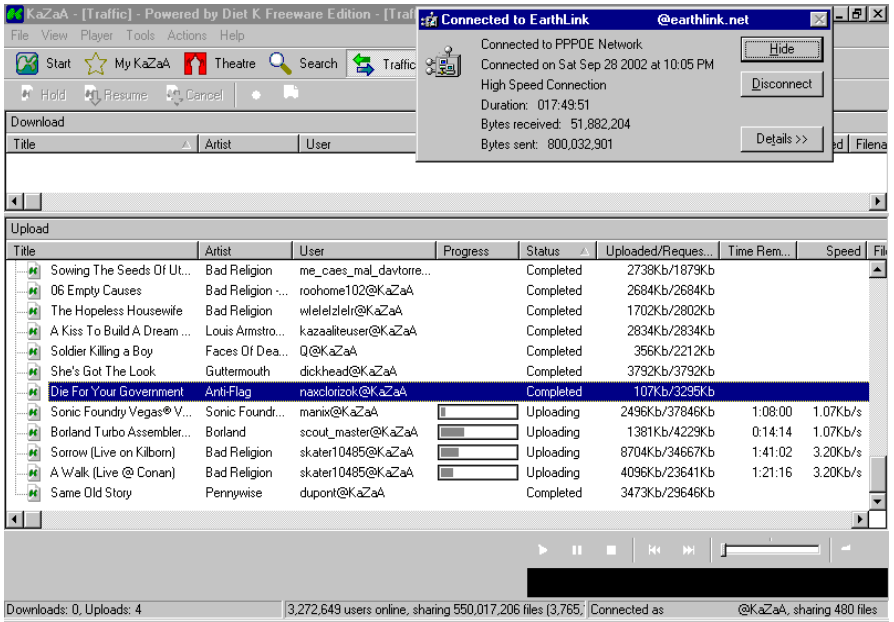
Release, Disclose, Or Alter Classified Information Without Consent

Relocate Information Systems Without Authorization

Share Personal Accounts And Passwords Or Permit The Use Of Remote Access

Prohibited Software

AR25-2


KaZaA - [Traffic] - Powered by Diet K Freeware Edition
Connected to EarthLink @earthlink.net
Connected to PPPOE Network
Connected on Sat Sep 28 2002 at 10:05 PM
High Speed Connection
Duration: 017:49:51
Bytes received: 51,882,204
Bytes sent: 800,032,901
Hide
Disconnect
Details >>
Download
Upload
Title Artist User Progress Status Uploaded/Reques... Time Rem... Speed
Sowing The Seeds Of Ut... Bad Religion me_caes_mal_davtorre... Completed 2738Kb/1879Kb
06 Empty Causes Bad Religion -... roohome102@KaZaA Completed 2684Kb/2684Kb
The Hopeless Housewife Bad Religion wlelelzlelr@KaZaA Completed 1702Kb/2802Kb
A Kiss To Build A Dream ... Louis Armstro... kazaaliteuser@KaZaA Completed 2834Kb/2834Kb
Soldier Killing a Boy Faces Of Dea... Q@KaZaA Completed 356Kb/2212Kb
She's Got The Look Guttermouth dickhead@KaZaA Completed 3792Kb/3792Kb
Die For Your Government Anti-Flag naxclorizok@KaZaA Completed 107Kb/3295Kb
Sonic Foundry Vegas® V... Sonic Foundr... manix@KaZaA Uploading 2496Kb/37846Kb 1:08:00 1.07Kb/s
Borland Turbo Assembler... Borland scout_master@KaZaA Uploading 1381Kb/4229Kb 0:14:14 1.07Kb/s
Sorrow (Live on Kilborn) Bad Religion skater10485@KaZaA Uploading 8704Kb/34667Kb 1:41:02 3.20Kb/s
A Walk (Live @ Conan) Bad Religion skater10485@KaZaA Uploading 4096Kb/23641Kb 1:21:16 3.20Kb/s
Same Old Story Pennywise dupont@KaZaA Completed 3473Kb/29646Kb
Downloads: 0, Uploads: 4
3,272,649 users online, sharing 550,017,206 files (3,765,
Connected as @KaZaA, sharing 480 files

P2P

Google Desktop

Portable Storage Device Security

Would You Drink A Soda That You Found Laying On The Street?

Don’t Stick Strange/Personal Portable Storage Devices In Your Government System

Protection

Concealment

Vigilance

How Do You Avoid Being A Victim?

- *When in doubt, talk to your Information Assurance (IA) personnel.*
  - The IA community is trained to deal with SE issues
- Don’t open attachments from anyone you don’t know
  - Opening an attachment can infect your computer
- Don’t provide personal information from unsolicited phone calls, visits, or emails.
  - Banks, travel agencies, the government do not send emails asking for personal information.
  - If you are unsure whether an email request is legitimate, try to verify it by contacting the agency directly. Do not use contact information provided on a web site connected to the request.

How Do You Avoid Being A Victim?

- If it's too good to be true it probably is. If you won a free trip to an exotic location you would have probably been notified by some other means then email.
  - Think about it. Are you really that lucky? Why would someone give you a free trip or cash? Use common sense. Clicking on a link in the email will provide the bad guys with your personal information
- Donating money or sending money to a "get rich quick" letter will result in you just losing your money.
  - Greed will get you every time. If you have too much money and just want to get rid of it, give it to your IA personnel, they can use some extra cash.

What Can You Do

- **Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic**
  - The Army keeps these tools updated, however remember to do this on your home computer.
- **Do not run programs of unknown origin**
  - Never download, install, or run a program unless you know it to be authored by a person or company that you trust.

What Can You Do

- **At a minimum, Digitally Sign Official E-mails**
  - **If your position involves official direct email contact with outside DoD entities, digital signatures might not be an option.**

- **Users should digitally sign and encrypt all messages that contain: (at a minimum)**
  - **For Official Use Only (FOUO)**
  - **Privacy Act / personal information**
  - **technical and contract data**
  - **proprietary information**
  - **foreign government information**
  - **financial information**
  - **source selection information**

- ***When in doubt, talk to your Information Assurance personnel.***
  - This should sound familiar

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information, report it to your IA personnel
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised.
  - Watch for any unexplainable charges to your account.
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission.
  - http://www.ftc.gov/

Social Engineering Reference Links

For additional information on social engineering, phishing, protecting your computer and personal information you can visit the following links:

- **Social Engineering Fundamentals**
  - http://www.securityfocus.com/infocus/1527
- **Social Engineering, the USB Way**
  - http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1
- **United States Law**
  - http://en.wikipedia.org/wiki/Social_engineering_(computer_security)#United_States_Law
- **Home Network Security**
  - http://www.cert.org/tech_tips/home_networks.html
- **Anti-Phishing Working Group**
  - **http://www.antiphishing.org/phishing_archive.html**

Remember

Contact Information

Your IA POC is:

USAMRMC IA

USAMRMCIA2@DET.AMEDD.ARMY.MIL